CLAIMS

1. A quantum key distributing method of correcting an error of reception data with probability information obtained as a result of measurement of photons on a quantum communication path to estimate original transmission data and using a result of the estimation as shared information, the quantum key distributing method comprising:

a first check-matrix generating step at which communication apparatus on a transmission side and a reception side individually generate a first parity check matrix (identical in the respective devices) optimized at a coding ratio in a desired range and extract a second parity check matrix (identical in the respective devices) corresponding to a specific coding ratio in the range from the first parity check matrix;

a first error-correction-information notifying step at which the communication apparatus on the transmission side notifies the communication apparatus on the reception side of first error correction information generated based on the second parity check matrix and the transmission data via a public communication path;

a first error correction step at which the communication apparatus on the reception side corrects an error of the reception data based on the first error correction information;

a second check-matrix generating step at which, when the error of the reception data is not completely corrected, the communication apparatuses on the reception side and the transmission side individually extract a third parity check matrix (identical in the respective devices) corresponding to a coding ratio lower than the last coding ratio from the first parity check matrix such that the last error correction information is a part of information at the time

of next error correction;

a second error-correction-information notifying step at which the communication apparatus on the transmission side notifies the communication apparatus on the reception side of additional second error correction information generated based on the third parity check matrix and the transmission data via the public communication path;

a second error correction step at which the communication apparatus on the reception side corrects the error of the reception data based on the first and the second error correction information; and

an encryption-key generating step of discarding a part of shared information according to an amount of error correction information laid open to the public and setting a result of discarding the part of the shared information as an encryption key when the error of the reception data is completely corrected in the processing at the first error correction step or when the error is completely corrected by repeatedly executing the processing at the second check-matrix generating step, the second error-correction-information notifying step, and the second error correction step.

2. The quantum key distributing method according to claim 1, wherein

the first parity-check-matrix generating process includes

a code-information determining step of determining a code length and a coding ratio in the desired range;

a fundamental-matrix generating step of selecting a matrix forming a basis of the first parity check matrix satisfying conditions that weights of rows and columns are

fixed and a number of cycles on a bipartite graph is equal to or larger than six and generating, based on the matrix, a first fundamental-matrix corresponding to an upper limit value in the range and a second fundamental-matrix corresponding to a lower limit value in the range;

a check-matrix generating step of generating a parity check matrix corresponding to the upper limit value of the coding ratio by optimizing, according to execution of Gaussian approximation based on the code length and the upper limit value, an order allocation of a weight of rows and a weight of columns of a parity check matrix corresponding to the upper limit value and dividing any one of a row weight and a column weight or both of the first fundamental-matrix based on the order allocation; and

an additional-matrix generating step of generating an additional matrix added to the parity check matrix corresponding to the upper limit value by optimizing, according to execution of the Gaussian approximation based on the lower limit value of the coding ration, an order allocation of a weight of rows and a weight of columns of a parity check matrix corresponding to the lower limit value under a constraint that a parity check matrix corresponding to the upper limit value is included and dividing any one of a row weight and a column weight or both of the second fundamental-matrix based on the order allocation, and

a parity check matrix corresponding to the lower limit value with the parity check matrix corresponding to the upper limit value and the additional matrix connected is set as the first parity check matrix.

3. The quantum key distributing method according to claim 1, wherein

the first parity-check-matrix generating process

includes

a code-information determining step of determining a code length and a coding ratio in the desired range;

a fundamental-matrix generating step of selecting a matrix forming a basis of the first parity check matrix satisfying conditions that weights of rows and columns are fixed and a number of cycles on a bipartite graph is equal to or larger than six and generating, based on the matrix, a fundamental-matrix corresponding to an upper limit value in the range and fundamental-matrixes corresponding to a plurality of coding ratios set stepwise in the range (including a fundamental-matrix corresponding to a lower limit value in the range);

a check-matrix generating step of generating a parity check matrix corresponding to the upper limit value of the coding ratio by optimizing, according to execution of Gaussian approximation based on the code length and the upper limit value, an order allocation of a weight of rows and a weight of columns of a parity check matrix corresponding to the upper limit value and dividing any one of a row weight and a column weight or both of the fundamental-matrix corresponding to the upper limit value based on the order allocation; and

an additional-matrix generating step of generating an additional matrix added to a parity check matrix corresponding to a coding ratio one stage higher by optimizing, according to execution of the Gaussian approximation based on a coding ratio one stage lower than a last coding ratio, an order allocation of a weight of rows and a weight of columns of a parity check matrix corresponding to the coding ratio under a constraint that a parity check matrix corresponding to the coding ratio one

stage higher is included and dividing any one of a row weight and a column weight or both of a fundamental-matrix corresponding to a coding ratio one stage lower based on the order allocation,

the additional-matrix generating step is repeatedly executed until the coding ratio reaches a coding ratio corresponding to the lower limit value while the coding ratio is lowered, and

a parity check matrix corresponding to the lower limit value with the parity check matrix corresponding to the upper limit value and all additional matrixes connected is set as the first parity check matrix.

4. The quantum key distributing method according to claim 2, wherein

a Euclidian geometric code is used as a matrix satisfying the conditions that weights of rows and columns are fixed and a number of cycles on a bipartite graph is equal to or larger than six.

5. The quantum key distributing method according to claim 3, wherein

a Euclidian geometric code is used as a matrix satisfying the conditions that weights of rows and columns are fixed and a number of cycles on a bipartite graph is equal to or larger than six.

6. A communication apparatus on a reception side that corrects an error of reception data with probability information obtained as a result of measurement of photons on a quantum communication path to estimate original transmission data and uses a result of the estimation as shared information to be shared with a communication

apparatus on a transmission side, the communication apparatus comprising:

a check-matrix generating unit that generates a parity check matrix optimized at a coding ratio in a desired range (hereinafter, "generated parity check matrix") and extracts a parity check matrix corresponding to a desired coding ratio in the range (hereinafter, "extracted parity check matrix") from the generated parity check matrix;

a decoding unit that corrects an error of the reception data based on the extracted parity check matrix (identical in the respective devices) and error correction information received from the communication apparatus on the transmission side via a public communication path; and

an encryption-key generating unit that discards a part of the shared information according to an amount of error correction information laid open to the public and uses a result of discarding the part of the shared information as an encryption key when an error of the reception data is completely corrected, wherein

the check-matrix generating unit extracts, when the error of the reception data is not completely corrected, parity check matrixes (identical in the respective devices) corresponding to respective code ratios from the generated parity check matrix until the error of the reception data is completely corrected such that last error correction information is a part of information at the time of next error correction and while lowering the coding ratio, and

the decoding unit corrects the error of the reception data based on error correction information added from the communication apparatus on the transmission side via the public communication path.

7. A communication apparatus on a transmission side that

uses, when a communication apparatus on a reception side estimates original transmission data from reception data with probability information obtained as a result of measurement of photons on a quantum communication path, a result of the estimation as shared information to be shared with the communication apparatus on the reception side, the communication apparatus comprising:

a check-matrix generating unit that generates a parity check matrix optimized at a coding ratio in a desired range (hereinafter, "generated parity check matrix") and extracts a parity check matrix corresponding to a desired coding ratio in the range (hereinafter, "extracted parity check matrix") from the generated parity check matrix;

an error-correction-information generating unit that generates error correction information based on the extracted parity check matrix and the transmission data and notifies the communication apparatus on the reception side of a result of the generation via a public communication path; and

an encryption-key generating unit that discards a part of the shared information according to an amount of error correction information laid open to the public and uses a result of discarding the part of the shared information as an encryption key when an error of the reception data is completely corrected, wherein

the check-matrix generating unit extracts, when the error of the reception data is not completely corrected, parity check matrixes (identical in the respective devices) corresponding to respective code ratios from the generated parity check matrix until the error of the reception data is completely corrected such that last error correction information is a part of information at the time of next error correction and while lowering the coding ratio, and

the error-correction-information generating unit notifies the communication apparatus on the reception side of additional error correction information via the public communication path until the error of the reception data is completely corrected.